A New Hybrid Approach for Infrastructure Discovery, Monitoring and Control

An enterprise IT infrastructure is a complex and a dynamic environment that is generally described as a black hole by its IT managers. The knowledge about an enterprise network’s layout (topology), resources (availability and usage), elements residing on the network (devices, applications, their properties and the interdependencies among them) as well as the ability to maintain this knowledge up-to-date, are all of critical for managing and securing IT assets and resources.

Unfortunately, the current available network discovery technologies (active network discovery and passive network discovery) suffer from numerous technological weaknesses which prevent them from providing with complete and accurate information about an enterprise IT infrastructure. Their ability to keep track of changes is unsatisfactory at best.

The inability to “know” the network directly results with the inability to manage and secure the network in an appropriate manner. This is since it is impossible to manage or to defend something, or against something, its existence is unknown or that only partial information about it exists.

The first part of the talk presents the current available network discovery technologies, active network discovery and passive network discovery, and explains their strengths and weaknesses. The talk highlights technological barriers, which cannot be overcome, with open source and commercial applications using these technologies.

The second part of the talk presents a new hybrid approach for infrastructure discovery, monitoring and control. This agent-less approach provides with real-time, complete, granular and accurate information about an enterprise infrastructure. The underlying technology of the solution enables maintaining the information in real-time, and ensures the availability of accurate, complete and granular network context for other network and security applications.

During the talk new technological advancements in the fields of infrastructure discovery, monitoring and auditing will be presented.
What this talk is about?

The success of any IT initiative depends on the availability of continuous, accurate and complete information about the IT infrastructure and the elements combining it. Without such information, any IT initiative is deemed to fail.

Many researchers have tried to solve the problem of knowing:

- What is on the enterprise network?
- Who is on the enterprise network?
- What is being done on the enterprise network?

Unfortunately they all have failed to answer these questions accurately and in a complete and granular fashion.

The ability of their methods to keep track of changes is unsatisfactory at best.
What this talk is about?

This talk discusses the strengths and weaknesses of current available network discovery technologies and why they fail to deliver

- Active Network Discovery
- Passive Network Discovery

Introduce a new agent-less, real-time approach for infrastructure discovery, monitoring and auditing, which provides with complete and accurate information about an enterprise IT infrastructure.

Ofir Arkin

CTO and Co-Founder, Insightix
http://www.insightix.com
Founder, The Sys-Security Group
http://www.sys-security.com
Computer Security Researcher
- Infrastructure Discovery
  - ICMP Usage in Scanning
  - Xprobe2 (The Active OS Fingerprinting Tool)
- VoIP Security
- Information Warfare

Member
- VoIPSA (Board member, chair security research committee)
- The Honeynet project

digital self defense
An Enterprise IT Network

Usually large, dynamic, and fairly complex
May contain several networks in different geographical locations
Hosts a variety of systems
Some systems are defined as mission critical:
  – Their availability is a must in order to perform the day to day computerized organizational tasks
  – Their unavailability will cause financial damages to the organization
  – The definition of what makes a system a mission critical one varies from one organization to another (i.e. networking equipment, servers, desktops, etc.)
An Enterprise IT Network

The regular operation of an enterprise network rely on a number of variables, such as:

- The availability of the IT network and its connectivity with other networks (i.e. B-2-B, the Internet, etc.)
- The availability of the elements residing on the IT network (i.e. network servers, network services, etc.)
- The ability of the elements residing on the IT network to operate and to function correctly
- The ability to maintain the integrity and confidentiality of corporate confidential information (i.e. core business assets)
- Other dependencies
An Enterprise IT Network

An IT organization must:
- Identify its network-based assets, their properties, their roles, and the interdependencies between them
- Determine the importance of its assets to the organization and to its business processes
- Provision its mission critical elements
- Know how its network(s) looks like
- Provision its network(s) (i.e. bandwidth consumption)
- Detect (immediately) and troubleshoot (fast) networking issues as they are introduced to the network
- Detect and eliminate elements on the network which pose a risk to the regular operation of the network and/or to its availability (or to the availability of one or more of the elements residing on the network)
- Detect changes made to the network
- Detect changes made to elements residing on the network
- Defend the core business assets
- Suffer from no network downtime (i.e. planning, provisioning, operational guidelines)
- Perform maintenance regularly (i.e. backups, upgrades of software and hardware, etc.)
- Prepare for the worse: Disaster Recovery Management (DRM)
- Perform other operations...
The Problem

The Required Information

To manage and to secure the IT infrastructure certain information about the enterprise IT network must be gathered and maintained up-to-date:

- Information about the network layout (topology)
- Information about the network resources (availability and usage)
- Information about the elements residing on the network (devices, applications, their properties, the interdependencies among them and their availability)

An intimate, complete and accurate knowledge of the networking environment is a must for network management and security systems in order to have an affect
The Problem

The information about an Enterprise IT network and its elements is either unavailable to IT managers or is partial, incomplete and inaccurate. A number of reasons contributes to this lack of knowledge:

- The type of information which needs to be collected and maintained is not easily produced
- There is a lack of corporate internal knowledge (in some cases only partial information about the IT environment is known)
- Information constantly changes (i.e. DHCP, user modifications, upgrades, etc.)
- The technologies used to gather the information are inappropriate

The Result

The inability to 'know the network' directly results with the inability to manage and to secure the Enterprise IT network in an appropriate manner. It is since it is impossible to manage or to defend something, or against something, its existence is unknown or that only partial information about it exists.
The Result

Existing network and security management systems an enterprise had deployed:
- Would work against 80% of the systems they should work against, where the remaining 20% are those systems which poses the highest risk to the availability and to the regular operation of the enterprise network and its elements
- Would never reach their full potential (since they would operate against only part of the systems they should and not against them all)
- Some management systems would receive incomplete and inaccurate information only to produce with more data which is inaccurate and incomplete

Current Available Network Discovery Technologies
Traditionally, in order to solve the issue of ‘knowing your network’ organizations have used a network discovery system.

Definition: A network discovery system should perform the discovery of the network topology, the elements residing on the network and their properties, and maintain this information up-to-date.

Current Available Technologies

The current available network discovery technologies:
– Active network discovery
– Passive network discovery

As we will illustrate the current available network discovery technologies suffer from numerous technological weaknesses which allows them to provide only with partial, incomplete, and sometimes inaccurate, information about an enterprise IT network.

Their ability to keep track of changes is unsatisfactory at best.
Active Network Discovery

ANDS Introduction

Active network discovery is a technology, which uses stimuli (packets) in order to provoke a reaction from network elements.

According to responses, or lack thereof, received from the queried network elements, knowledge about a network and its elements will be gathered.

digital self defense
ANSDS Introduction

The information an ANSDS attempts to collect may include the following:
– An inventory of network elements and their properties
– Information on network services and their version
– Configuration related information of a network and/or of its elements
– Topology related information*
– Vulnerability analysis related information*

* Not every active network discovery system provides vulnerability analysis information

ANSDS Deployment

digital self defense
Traditionally, an active network discovery system (ANDS) queries its targets from a single location on the network, where it is installed. An ANDS may operate using one (or more) operational ways:

- Query only the local IP subnet to which it is attached
- Receive a manual list of IP addresses and/or IP subnets against which to operate
- Start by querying the local IP subnet to which it is attached, and then querying remote IP subnets after learning about their existence using information extracted from local routers or other elements on the local IP subnet.

Active Network Discovery Strengths
ANDS Strengths

An ANDS query network elements for specific parameter values needed for the active network discovery process.
The initiation of an active network discovery scan or a specific query can be controlled (an ANDS may allow complete control over the parameter values to query for, and the time to perform the queries).
The pace of an active network discovery scan can be controlled.
An active network discovery scan is able to cover the entire IP address range of an enterprise.

Active Network Discovery Weaknesses

digital self defense
**ANDS Weaknesses**

**Incomplete Discovery**
- An ANDS will detect network elements, which will be operational (‘up’) on a network at the time of the discovery. This is if the packets sent by an ANDS are able to reach the probed elements, and that the probed elements answer the type of query sent.
- Network obstacles such as network firewalls, host based firewalls, load balancers, NAT devices, etc. will prevent, in many cases, probe packets from reaching their target network elements.
- A good example would be of Microsoft Windows XP running service pack 2.

**Information Enumeration Failure**
- An ANDS may need to enumerate configuration information from a number of network elements found on a probed network.
- This process depends on the availability, and the willingness to communicate, of certain network services that need to operate on the queried network elements.
- The inability to extract the required configuration information would harm the active network discovery process, and would result in partial knowledge gathered, and incomplete discovery.
- Examples: SNMP, Windows Remote Registry Service.
ANVS Weaknesses

Non Real-Time
- Slow
- Time-consuming process
- A considerable amount of time is required to probe network elements, and to collect and process the probe replies received
- Produces only a snapshot of a network and its elements at a certain point in time

ANVS Weaknesses

Network Performance Degradation
- Consumes a significant amount of network bandwidth
- The amount of network bandwidth consumed is directly affected by the number of IP addresses scanned
- The act of active network discovery may slow down the operation of networking devices, which are present on the path between an ANVS to its probed network elements, by overloading them with a considerable amount of network traffic, which needs to be processed
- Actively scanning a large number of network elements may cause a considerable slow down in a network’s performance and operation
ANDS Weaknesses

Scanning at Off-Pick Hours
- The information collection process performed by an ANDS, might take a considerable amount of time to complete and may exceed the window of time for the off-peak network operation hours
- Many systems might be offline at the time the active network discovery is to be performed
- In some cases it is impossible to define off-peak hours. For example, different business processes operates at different times during the day

ANDS Weaknesses

A Faster Scan, a Higher Risk
- The attempt to compensate for the slowness of the active network discovery process by increasing the pace of the scan may result in other consequences
- Increasing the pace of the active network discovery process means that more probe packets will be sent per a certain timeframe
- A networking element, such as a switch, which can handle a certain amount of packets per second, will selectively drop packets or even crash if the actual number of packets per second that the networking element would be required to process is higher than it can handle
- This is exactly the case when a large number of IP addresses are to be scanned in a very short time period
ANS Weaknesses

Stability Issues with Scanned Network Elements

- It is a known fact that some ANDSs may introduce a denial-of-service condition (i.e. a reboot, a crash) to some network elements when they probe them for information. This is either due to:
  - The pace of the scan and the number of packets sent to a network element during an active network discovery process
  - The usage of non-RFC compliant probe packets, which some probed network elements cannot withstand due to their unexpected input
  - Performing information enumeration against a network element where the output produced by the network element overwhels the network element and disrupts its service (i.e. arp cache tables with routers)
  - Performing vulnerability analysis against discovered network elements by using real-world exploitation attempts which may introduce a denial-of-service condition to some network elements

Stability Issues with Networking Devices

- One form of a denial of service condition may occur if a networking element on the path between an ANDS and its targets would be required to process a higher number of packets per second than it can handle due to an increase in the number of packets which needs to be processed as a result of an active network discovery process

- Examples:
  - Switches
  - Firewalls (i.e. state tables)
'Active Scan Free' Networks

- In some organizations certain corporate networks cannot be actively probed
- This is because the effect of running an active network discovery processes against these networks cannot be predicted or is believed to cause disruptions with the regular operation of the network and/or its elements
- Usually these networks contain mission critical systems, in which case a downtime to one of these systems would cause significant lost of revenue to the organization
- The problem resulting is the inability to determine the contents and the level of (in)security
In order to try to solve some of the weaknesses of active network discovery, vendors are distributing the scan among multiple systems.

Two main operational ways exist for distributed scanning:

- Clusters
- Proxies
Active Network Discovery Clusters

Unfortunately, running an ANDS in a cluster mode has no real advantage:

- The network is still scanned from a single location
- The network might get saturated faster since there are multiple machines scanning the network at the same time
- The risk for an instability with network devices on the path between an ANDS cluster and its targets is higher since more packets are generated in the same amount of time
- Using an ANDS cluster would not always speed the discovery
- All other weaknesses still apply

Active Network Discovery Proxies

digital self defense
Active Network Discovery Proxies

Advantages over the traditional ANDS:
- In many cases active network discovery packets would not pass through routers and firewalls, thus limiting the affect of the load of the scan contained only to the local network(s) they are scanning
- The scan time using active network discovery proxies should be faster, since the scan is performed at the same time by different proxies targeting different IP subnets

An ANDS Proxy still has substantial disadvantages:
- Pre-knowledge about the discovered network(s) is required prior to deploying active network discovery proxies
- If there are IP subnets or networks which are unknown they will remain unknown
- Scan packets may still cause instabilities with scanned network elements and networking equipment
- An ANDS proxy can bring its local network down if it is misconfigured
- The fact that an active network discovery proxy needs to be installed per subnet or subnets makes it a difficult administrative issue (more moving parts, co-operation of different groups)
- All other weaknesses still apply
Passive network discovery is a technology, which processes captured packets from a monitored network in order to gather information about the network, its active elements and their properties. It relies on user and network activities in order to draw conclusions about the network, its active elements and their properties. It is usually installed at a network chokepoint of the network. The roots of passive network discovery and monitoring technology go back to the mid-1990s where references regarding the usage of the technology can be found.
PNDS Deployment (1/4)

PNDS Deployment (2/4)

digital self defense
PNDS Deployment (3/4)

digital self defense
PNDS Introduction

Information collected using a PNDS may include the following:
- Active network elements and their properties (i.e. underlying operating system)
- Active network services and their versions
- To ascertain the distances between active network elements and the monitoring point on the network*
- Active client-based software and their versions
- Network utilization information
- Vulnerabilities found for network elements residing on the monitored network*

* Not every passive network discovery system provides these features

The information collected by a PNDS might be used for the following purposes:
- Building the layer-3 based topology of a monitored network
- Auditing
- Providing network utilization information
- Performing network forensics*
- Performing vulnerability discovery*
- Create a context regarding the network operation
- Feeding information collected into other security and/or network management systems (contextual information)

* Not every passive network discovery system provides these features
Passive Network Discovery Strengths

Real-Time
Has zero impact over the performance of the monitored network*
Does not pose a risk to the stability of a monitored network to gather information from all TCP/IP layers of network traffic processed
Detection of Active network elements and their properties
- Detect active network elements which transmit and/or receive data over the monitored network
- Detect network elements as they become active and transmit and/or receive data over the monitored network
- Detect network elements which have low uptime
- Detect network elements which may transmit or receive data for short time periods only
PNDS Strengths

Detection of certain properties related to the network monitored and to its elements:

- Detect on which network elements active network services are operational and serving requests
- Detect active network services running on non-default ports
- Detect active client-based network software operating on network elements on the monitored network

Detection of elements behind ‘network obstacles’

- Detect network elements behind packet filtering devices
- Discover NAT enabled devices

Granular network utilization information
Able to detect network related abnormalities*

In the case an enterprise may have ‘active scan free’ networks, passive network discovery can be used as a solution

Passive Network Discovery
Weaknesses
PNDS Weaknesses

What you see is only what you get

- A PNDS cannot draw conclusions about an element and/or its properties if the related network traffic does not go through the monitoring point
- Information which needs to be collected by a passive network discovery and monitoring system may never be gathered due to a lack of network activity which discloses the information
- A PNDS cannot detect idle (not active) elements, services, and applications
- The discovery performed by a PNDS will be partial and incomplete, since it is unable, technologically, to detect all network assets and their respected properties

PNDS Weaknesses

Passive network discovery cannot detect

- All assets
- All protocols and services
- All ports

The quality and relevancy of network traffic observed

- No control over the type of information, which would pass through the monitoring point
- Information which needs to be collected may never be gathered due to a lack of network activity which discloses the information
- Lack of the ability to have granularity with the detected information
PNDS Weaknesses

No control over the pace of the discovery
Limited IP address space coverage
Not everything can be passively determined

- In some cases information cannot be unveiled using a passive network discovery system. For example, passive vulnerability discovery, were not all vulnerabilities can be passively determined

Incomplete and partial network topology

- Would gather network topology information based on the distances discovered between network elements and the monitoring point
- Rely on the time-to-live field value with the IP header of observed network traffic
- Provides with network topology information which relates only to layer-3 based information
- Cannot detect the physical network topology of a network it is monitoring
  - It cannot detect the network switches, which operated on the network (usually a network switch will not generate network traffic other then the spanning tree protocol to its adjunct switches only)
  - Cannot query switches for their CAM tables detecting which network element (or elements) is connected to which switch port

digital self defense
PNDS Weaknesses

Incomplete and partial network topology (continued)
- It cannot uncover routing done not through its monitoring point
- It cannot detect other routers operating on the monitored network
- It is unable to uncover all of the network assets operating on the monitored network
Deployment location and the number of sensors needed
- The deployment location of the monitoring system determines the network traffic's data quality it will be receiving.
- The quality is maximized when the deployment location is as close as possible to the access layer (i.e. between layer-2 to layer-3).
- A passive network discovery and monitoring system loses some of its information collection abilities when it is not observing layer-2 based traffic.
- A number of passive network discovery and monitoring system are to be deployed in an enterprise implementation in order to have a complete coverage of the enterprise networks and to allow the highest quality of network data to be collected.
PNDS Weaknesses

No service monitoring
- Cannot monitor the state of network services
- Cannot uncover change transitions
- Cannot uncover ‘idle’ network services

Passive Network Discovery
The Less Obvious Weaknesses

digital self defense
PNDS Weaknesses

Cannot Resist Decoy and Deception
- A PNDS gathers data based on information extracted from network traffic
- It may be possible to trick a PNDS into making the wrong conclusions about a network and its elements by poisoning the network traffic
- A PNDS can be tricked since it is unable to validate the information collected from a monitored network
- The location, and the distance, a PNDS is from a monitored network would determine the level of confidence the results it will produce would be

PNDS Weaknesses

Cannot Resist Decoy and Deception (Continued)
- Influencing the accuracy of a PNDS might influence other systems which rely on the data collected by the PNDS as their input
- A good example would be of PNDSs that are used to accompany other products such as NIDS, NIPS, etc.
- The result would be of a management system producing inaccurate, and incomplete conclusions about the network and its elements fooling its users into believing they are in control, and with sufficient information about their network where the truth is, they are missing key elements, and cannot identify issues which might bring their networks to a complete halt
PNDS Weaknesses

digital self defense
PNDS Weaknesses

Denial of Service
- “Snort TCP/IP Options Bug Lets Remote Users Deny Service”, Marcin Zgorecki, post to Snort-devel mailing list, October 2004
- “Unknown vulnerability in the Gnutella dissector in Ethereal 0.10.6 through 0.10.8 allows remote attackers to cause a denial of service (application crash)”, CAN-2005-0009, http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0009

Remote Code Execution
- “Buffer overflow in the X11 dissector in Ethereal 0.8.10 through 0.10.8 allows remote attackers to execute arbitrary code via a crafted packet”, CAN-2005-0084, http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0084
- “Ethereal 0.10.10 SIP Dissector Overflow”, May 8th, 2005, http://www.securitylab.net/ethereal-0-10-10.txt
The Research

The Research Background

Came from an identified need
Conducted over the past several years
During the course of the research, the current network discovery technologies were analyzed and their strengths and weaknesses examined
The research included theoretical analysis, and a variety of test beds (lab experiments, and real-world deployments)
Strict goals were set
The Research Background

Goals for the research of a new network discovery technology were:
– Complete and Accurate
– Real-Time
– Agent-less
– To be safe to execute against production environments
– Detect and react to changes in real-time
– Draw a physical network topology map
– Provide with strong audit capabilities
– Provide with granular network utilization information
– Resist decoy and deception
– Cover the entire IP range of an enterprise network

The Research Results

During the research I have learned that:
– Many theoretical techniques published in the recent years are not able to be executed in the real world of IT networks
– They either cover only a portion of a problem, or are completely mistaken with their assumptions
DID* Introduction

Dynamic infrastructure discovery is a network discovery technology which overcomes the limitations of current available network discovery technologies by tightly integrating between active and passive network discovery.

It enjoys new discovery abilities and it is adjustable to any networking environment (automatically balances the usage between passive and active network discovery).

* A system using DID technology may be termed as DNDS (Dynamic Network Discovery System)
DID Introduction

Information collected using a DNDS may include the following:

- Network elements and their properties (i.e. underlying operating system)
- Network services and their versions
- Network topology (physical)
- Communications between network elements*
- Active client-based software and their versions
- Granular network utilization information
- Vulnerabilities found for network elements residing on the monitored network
- Any piece of information which can be either gathered passively or actively

* Only if those are passing through the monitoring point
DID Introduction

The information collected by a DNDS might be used for the following purposes:

- Complete and accurate asset discovery
- Mapping the physical network topology (i.e. hosts, routers, switches, hubs)
- Real-time change detection mechanism
- Extensive Auditing platform (i.e. communications between elements, opened network services*, device properties)
- Creating a context regarding the network and its operation
- Providing granular network utilization information
- Feeding information collected into other security (i.e. vulnerability assessment*) and/or network management (Asset management, CMDB) systems (contextual, accurate and up-to-date information)
- Conclusions about the network and/or its elements can be made according to information gathered by both information gathering methods

Dynamic Infrastructure Discovery

Strengths

digital self defense
DID Strengths

Real-time
Complete (detect all devices)
Agent-less
Validate information gathered (resist decoys)
Provides with granular information
Real-time change detection (i.e. topology related changes, an element’s properties, etc.)
Enjoys new discovery abilities driven from the tight integration between the network discovery technologies (i.e. VMware host and its guests)

DID Strengths

Controls every aspect of the discovery (time, pace, information, targets)
Does not pose risk to the network operation (active probing is done in a surgical manner)
Granular network performance information (per network, per application, per host)
Overcomes all of the limitations of current available network discovery technologies
Dynamic Infrastructure Discovery Weaknesses

DID Weaknesses

Not all idle listening services may be detected actively
Questions?

Resources

Thanks!